

U.S. APPLICATION NO. 09/993,163

Title: CASHLESS TRANSACTION
CLEARINGHOUSE

Filed: November 16, 2001

Inventors: Michael OBERBERGER
Richard Rowe

Attorney Docket No.: IGT1P035X1/
P-311CIP

PENDING CLAIMS:

1. A cashless instrument transaction network for generating cashless transactions between a plurality of separate gaming properties, each of which generates and validates cashless instruments, the cashless instrument transaction network comprising:

a cashless instrument transaction clearinghouse, the cashless instrument transaction clearinghouse comprising:

(i) a network interface allowing the cashless instrument transaction clearinghouse to communicate with each of the separate gaming properties; and

(ii) a processor configured or designed to (a) receive cashless instrument validation requests via the network interface from a first property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property (b) send information, via the network, to the second property requesting the second property to approve or reject the cashless instrument validation request;

at least one cashless gaming device, located at each of the plurality of separate gaming properties, that communicates with cashless instrument clearinghouse; and

a network allowing communication between the cashless instrument clearinghouse and the cashless gaming devices.

2. The cashless transaction network of claim 1, wherein the cashless transaction clearinghouse further comprises a memory device that stores cashless gaming device public encryption keys for each of the cashless gaming devices.

3. The cashless transaction network of claim 2, wherein the processor is further designed or configured 1) to decrypt cashless transaction information encrypted with a

cashless gaming device private encryption key using a corresponding cashless gaming device public encryption key and 2) to encrypt cashless transaction information using the public encryption keys.

4. The cashless transaction network of claim 1, wherein the cashless transaction clearinghouse further comprises a memory device that stores a clearinghouse private encryption key.

5. The cashless transaction network of claim 4, wherein the processor is further designed or configured 1) to decrypt cashless transaction information encrypted with a clearinghouse public encryption key using the clearinghouse private encryption key and 2) to encrypt cashless transaction information using the clearinghouse private encryption key.

6. The cashless transaction network of claim 1, wherein the gaming devices further comprise a memory device storing a clearinghouse public encryption key and a gaming device private encryption key.

7. The cashless transaction network of claim 6, wherein the gaming devices encrypts cashless transaction information using the clearinghouse public encryption key and decrypts cashless transaction information encrypted with a clearinghouse private key using the clearinghouse public encryption key.

8. The cashless transaction network of claim 6, wherein the gaming device encrypts cashless transaction information using the gaming device private encryption key and decrypts cashless transaction information encrypted with a gaming device public encryption key using the gaming device private encryption key.

9. The cashless transaction network of claim 1, wherein the cashless gaming devices encrypt and decrypt cashless transaction information.

10. The cashless transaction network of claim 1, wherein the processor is further designed or configured to encrypt and decrypt cashless transaction information.
11. The cashless transaction network of claim 1, wherein the network comprises a local area network, a wide area network, the Internet, a private intranet and combinations thereof.
12. The cashless transaction network of claim 1, wherein the cashless gaming device is selected from the group consisting of a gaming machine, a hand-held computing device, a clerk validation terminal and a cashless server.
13. The cashless transaction network of claim 1, wherein the processor is further designed or configured to allow promotional credits issued to a cashless instrument at a first gaming property to be used for game play at a second gaming property.
14. A method in an cashless instrument transaction clearinghouse of communicating with a plurality of gaming properties each of which generates and validates cashless instruments, the method comprising:
- sending a clearinghouse public encryption key to a cashless gaming device at each of the plurality of gaming properties wherein the clearinghouse public encryption key is part of a public-private encryption key pair generated at the clearinghouse;
 - receiving a public encryption key from a gaming device at each of the plurality of gaming properties wherein each public encryption key is a part of a public-private encryption key pair generated at each property;
 - authenticating a sender of each of the public encryption keys received at the clearinghouse;
 - generating a message for each property wherein the message includes information at least encrypted with the property's public encryption key and a clearinghouse private encryption pair that is part of the public-private encryption key pair generated at the clearinghouse; and
 - sending the message to each property

wherein the cashless instrument transaction clearinghouse at least (i) receives cashless instrument validation requests from a first property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and (ii) sends information to a second gaming property requesting the second property to approve or reject the cashless instrument validation request..

15. A method in an cashless instrument transaction clearinghouse of communicating with a plurality of gaming properties each of which generates and validates cashless instruments, the method comprising:

- receiving a first message addressed to a second property from a first property wherein the message includes encrypted cashless transaction information;
- authenticating an identity of the first message sender;
- decrypting the encrypted cashless transaction information;
- identifying an address for the second property;
- encrypting the cashless transaction information for second message addressed to the second property; and
- sending the second message with the encrypted cashless transaction information to the second property;

wherein the cashless instrument transaction clearinghouse at least (i) receives cashless instrument validation requests from a first property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and (ii) sends information to a second gaming property requesting the second property to approve or reject the cashless instrument validation request.

16. The method of claim 15, further comprising:
operating on the cashless transaction information.

17. The method of claim 15, further comprising:
storing the cashless transaction information.

18. The method of claim 15, further comprising:
translating the cashless transaction information from a first format used by the first property to a second format used by the second property.
19. The method of claim 15, wherein the cashless information in the first message is encrypted with a symmetric encryption key.
20. The method of claim 15, wherein the cashless transaction information in the first message is encrypted using a public-private encryption key pair.
21. The method of claim 15, wherein the first message includes an encrypted symmetric encryption key.
22. The method of claim 21, further comprising:
decrypting the symmetric encryption key.
23. The method of claim 21, wherein the symmetric encryption key is encrypted at the first property using a public-private encryption key pair.
24. The method of claim 21, wherein the symmetric encryption key is encrypted twice at the first property using a first property private encryption key from a first public-private encryption key pair and using a clearinghouse public encryption key from a second public-private encryption key pair.
25. The method of claim 24, wherein the symmetric encryption key is decrypted at the clearinghouse using a first property public encryption key from the first public-private encryption key pair and is decrypted using a clearinghouse private encryption key from the second public-private encryption key pair.
26. The method of claim 25, wherein the cashless transaction information for the second message is encrypted with a symmetric encryption key.

27. The method of claim 15, wherein the cashless transaction information for the second message is encrypted using a public-private key pair.
28. The method of claim 15, further comprising:
generating a first symmetric encryption key;
encrypting the cashless transaction information for the second message with the first symmetric encryption key;
encrypting the first symmetric encryption key; and
generating the second message with the encrypted first symmetric encryption key and the encrypted cashless transaction information.
29. The method of claim 28, wherein the first symmetric encryption key is encrypted at the clearinghouse using a clearinghouse private encryption key from a first public-private encryption key pair and using a public encryption key from a second public-private encryption key pair.
30. The method of claim 28, further comprising:
receiving from the second party a third message comprising at least encrypted cashless transaction information and an encrypted second symmetric encryption key;
decrypting the second symmetric encryption key
and comparing the second symmetric encryption key to the first symmetric encryption key to authenticate the message sender.
31. The method of claim 15, further comprising:
receiving from the second party a third message and
authenticating the message sender.
32. A method in a first cashless gaming device located at a first gaming property which generates and validates cashless instruments of communicating instruments via a cashless instrument transaction clearinghouse with a second cashless gaming device

located at a second gaming property which generates and validates cashless, the method comprising:

generating cashless transaction information;

encrypting the cashless transaction information; and

sending a first message addressed to the second gaming property with at least the cashless transaction information to the cashless transaction clearinghouse

wherein the cashless instrument transaction clearinghouse at least (i) receives cashless instrument validation requests from a first property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and (ii) sends information to a second gaming property requesting the second property to approve or reject the cashless instrument validation request.

33. The method of claim 32, further comprising:

generating the first message.

34. The method of claim 32, wherein the gaming device is selected from the group consisting of a gaming machine, a cashless server, a hand-held computing device and a clerk validation terminal.

35. The method of claim 32, wherein the cashless transaction information is encrypted with one or more of a symmetric encryption key, a public encryption key of a public-private encryption key pair, a private encryption key of a public-private encryption key pair and combinations thereof.

36. The method of claim 32, further comprising:

receiving a second message from the cashless instrument transaction clearinghouse; and

authenticating a sender of the second message.

37. The method of claim 36, further comprising:

decrypting cashless transaction information included in the second message.

38. The method of claim 37, wherein the information is decrypted with one or more of a symmetric encryption key, a public encryption key of a public-private encryption key pair, a private encryption key of a public-private encryption key pair and combinations thereof.

39. The method of claim 32, further comprising:
generating a symmetric encryption key and
encrypting the cashless instrument information with the symmetric encryption key.

40. The method of claim 39, further comprising:
encrypting the symmetric encryption key ;
generating a second message with the encrypted symmetric encryption key and the encrypted cashless instrument information;
and sending the second message to the cashless instrument transaction clearinghouse.

41. A method in a cashless gaming device of authenticating a public encryption key from a cashless transaction instrument clearinghouse, the method comprising:
generating a symmetric encryption key using a seed shared with the clearinghouse;
encrypting a first information sequence with the symmetric encryption key;
sending a first message with the encrypted first information sequence to the clearinghouse;
receiving a second message with an encrypted second information sequence and encrypted clearinghouse public encryption key from the clearinghouse;
decrypting the second information sequence with the symmetric encryption key;
and
authenticating the sender of the second message using the first information sequence and the second information sequence

wherein the cashless instrument transaction clearinghouse at least (i) receives cashless instrument validation requests from a first gaming property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and (ii) sends information to a second gaming property requesting the second property to approve or reject the cashless instrument validation request.

42. The method of claim 41, further comprising:
decrypting the clearinghouse public encryption key with the symmetric encryption key and
storing the clearinghouse public encryption key.
43. The method of claim 41, further comprising:
comparing the first information sequence to the second information sequence.
44. The method of claim 41, further comprising:
receiving the seed from the clearinghouse.
45. The method of claim 41, further comprising:
generating the first message.
46. The method of claim 41, further comprising:
encrypting information with the clearinghouse public encryption key and
sending a message with the encrypted information to the clearinghouse.
47. The method of claim 41, wherein the first information sequence is a random noise sequence.
48. The method of claim 41, wherein the cashless instrument is selected from the group consisting of a smart card, a debit card, a bar-coded ticket and an EZ pay ticket voucher.

49. The method of claim 41, wherein the first information sequence and the second information sequence are identical.

50. A method in a cashless instrument transaction clearinghouse of sending a public encryption key to a cashless gaming device, the method comprising:

- generating a symmetric encryption key using a seed shared with the cashless gaming device;

- receiving a first message with an encrypted information sequence from the cashless gaming device;

- decrypted the information sequence with the symmetric encryption key;

- encrypting the information sequence with the symmetric encryption key;

- encrypting a clearinghouse public encryption key with the symmetric encryption key; and

- sending a second message, with (i) the information sequence encrypted with symmetric encryption key and (ii) the public encrypted key encrypted with the symmetric encryption key, to the clearinghouse;

- wherein the cashless instrument transaction clearinghouse at least (i) receives cashless instrument validation requests from a first gaming property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and (ii) sends information to a second gaming property requesting the second property to approve or reject the cashless instrument validation request.

51. The method of claim 50, wherein the information sequence is a random noise sequence.

52. The method of claim 50, wherein the cashless instrument is selected from the group consisting of a smart card, a debit card, a bar-coded ticket and an EZ pay ticket voucher.

53. The method of claim 50, further comprising:
generating a encryption key pair including the clearinghouse public key and a clearinghouse private key.
54. The method of claim 50, further comprising:
generating the second message.
55. A method in a cashless gaming device of sending a public encryption key to a cashless instrument transaction clearinghouse and authenticating the public encryption key has been received by the clearinghouse, the method comprising:
generating a symmetric encryption key using a seed shared with the clearinghouse;
encrypting a cashless gaming device public encryption key with the symmetric encryption key;
encrypting the cashless gaming device public encryption key with a clearinghouse public encryption key;
sending a first message with the doubly encrypted cashless gaming device public encryption key to the clearinghouse;
receiving a second message with an encrypted information sequence;
decrypting the information sequence with the clearinghouse public encryption key;
decrypting the information sequence decrypted with clearinghouse public encryption key with the symmetric encryption key; and
authenticating the sender of the second message using the cashless gaming device public encryption key and the information sequence
wherein the cashless instrument transaction clearinghouse at least (i) receives cashless instrument validation requests from a first gaming property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and (ii) sends information to a second gaming property requesting the second property to approve or reject the cashless instrument validation request.

56. The method of claim 55, further comprising:
comparing the information sequence to the cashless gaming device public encryption key.
57. The method of claim 55, wherein the information sequence and the cashless gaming device public encryption key are identical.
58. The method of claim 55, further comprising:
generating an encryption key pair including the cashless gaming device public key and a cashless gaming device private key.
59. The method of claim 55, further comprising:
generating the first message.
60. The method of claim 55, further comprising:
receiving the seed from the clearinghouse.
61. The method of claim 55, further comprising:
receiving the clearinghouse public encryption key from the clearinghouse.
62. The method of claim 61, further comprising:
authenticating an identity of the sender of the clearinghouse public encryption key.
63. A method in a cashless instrument transaction clearinghouse of receiving a public encryption key from a cashless gaming device and authenticating an identity of the cashless gaming device, the method comprising:
generating a symmetric encryption key using a seed shared with the cashless gaming device;
receiving a first message with an encrypted cashless gaming device public encryption key from the cashless gaming device;

decrypting the information sequence with the symmetric encryption key;
decrypting the cashless gaming device public encryption key with the symmetric encryption key;
decrypting the cashless gaming device public encryption key with a clearinghouse private encryption key;
encrypting the cashless gaming device public encryption key with the clearinghouse public encryption key;
encrypting the cashless gaming device public encryption key encrypted with the clearinghouse public encryption key with the symmetric encryption key; and
sending a second message with the doubly encrypted cashless gaming device public encryption key to the clearinghouse;
wherein the cashless instrument transaction clearinghouse at least (i) receives cashless instrument validation requests from a first gaming property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and (ii) sends information to a second gaming property requesting the second property to approve or reject the cashless instrument validation request.

64. The method of claim 63, further comprising:

storing the cashless gaming device public encryption key.

65. The method of claim 63, further comprising:

sending information encrypted with the cashless gaming device public encryption key to the cashless gaming device.